Exhibit to Data Center Services Service Component Provider Master Services Agreement

DIR Contract No. DIR-DCS-SCP-MSA-002

Between

The State of Texas, acting by and through the Texas Department of Information Resources

and

Atos IT Governmental Outsourcing Services, LLC (formerly called XBS Disposition Subsidiary Two, LLC)

Appendix 20 to Eleventh Amendment of Attachment 8-B Services Solution Document

Functional Area: "Service Integration & Orchestration**"**

May 31, 2016

Table of Contents

1 Disclaimer:

This document is provided as a proposed roadmap and strategic outline. This document is not a contract, nor does it convey any contractual obligations.

2 HCI Document References:

This Services Solution Document (SSD) refers to key functionality, solutions and services described in other documents, as follows:

- **SSD – Hybrid Cloud, version P1 D1.11**
    - Section 1 (page 1) – TxDCS Hybrid Cloud (introduction of TxDCS Hybrid Cloud)
    - Section 1 (page 2) – High Level Architecture (HLA)
- **SSD – Hybrid Cloud Infrastructure – Network, version P1.D16.**
    - Section 4.3.2.1 Virtual Data Center overview (“VDC”, also identified as “VMDC”)
- **SSD – Hybrid Cloud Orchestration, version P1 D1.14**
    - Section 1 – introduction to the Enterprise Service Bus
    - Section 1 – introduction to the NIS definition of secure cloud provider
- **SSD - Hybrid Cloud Orchestration-DCS Optimization** 17-Sep-2015 vInfraResponse.
    - Section 2.2 – further details on ESB implementation and tools integration

The TxDCS Hybrid Cloud is defined in the Hybrid Cloud SSD document, version P1 D1.11 – here is a summary:

At its core, the TxDCS program provides customers private cloud IaaS hosting for Intel and UNIX compute needs. In addition the private cloud IaaS has access to dedicated tiered storage solutions housed within the Texas Consolidated Datacenters (CDC). It is the Service Provider’s intent to extend to and integrate with key partners in the public cloud sectors to create the TxDCS Hybrid Cloud (TxHC). These additional cloud services may be accessed as a part of an integrated platform or software service directly from the secure CDC datacenter backbone network or from local/regional offices using a hybrid cloud gateway appliance.

3 Executive Summary

Over the past several years, TxDCS and its IT partners have been effectively driving to standardize processes across the organization, providing more visibility and predictability to the quality and performance of services, and being more proactive and service-aligned with business needs. However, this is now no longer enough. With the pressures of ever increasing business velocity, the proliferation of cloud resources at affordable prices, the change in the dev/op paradigm for self-service and rapid testing and deployment, as well as the inexorable drive towards the goal of 100% availability and predictability of services, TxDCS and its IT partners have embarked on a strategy to drive to the next level of the Operational Maturity Model.

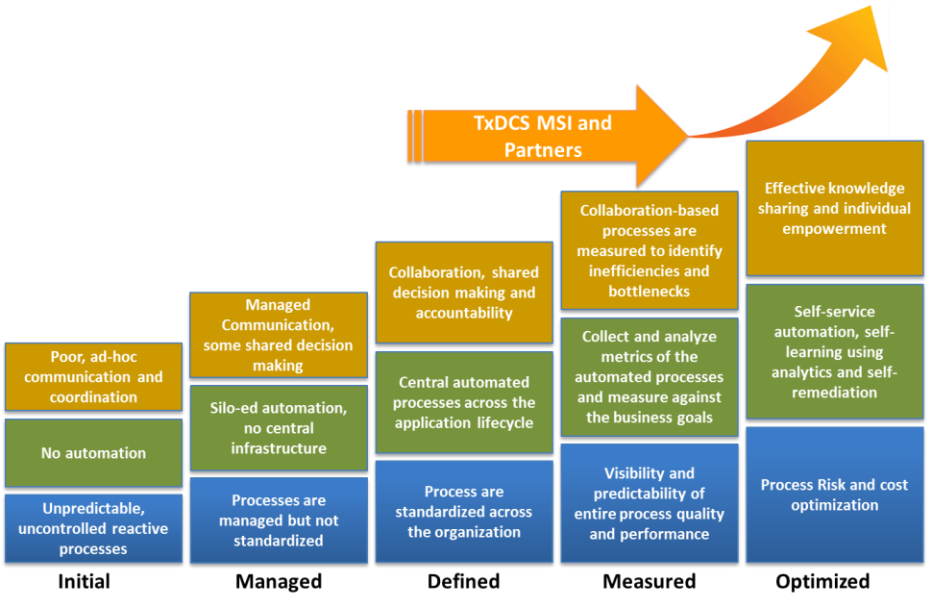


Fig 1: Operational Maturity Model

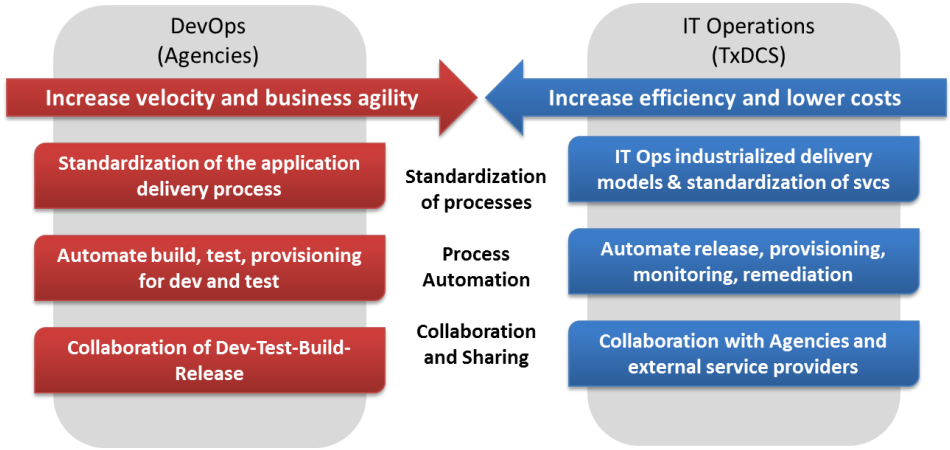
Today, TxDCS and its partners have made great progress along the Operational Maturity Model, moving from the "Defined" phase into the "Measured" phase. An existing challenge for IT operations is "IT industrialization" - applying manufacturing best practices to IT processes in order to optimize the cost and speed of service delivery. One of the key tenets of the lean manufacturing practices is standardization and automation of the service delivery processes related to all phases of the lifecycle – from request, approval to fulfillment. This direction is aligned with the IT Operations Maturity Model.

In order to achieve mass production, IT Operations needs to automate its processes, such as release of changes, resource provisioning, monitoring, incident resolution, remediation of problems, etc.

Increasing business agility requires different levels of collaboration between IT Operations, and business and development teams, in order to optimize speed versus risk. TxDCS IT is transformed into a facilitator and "enabler", providing guidance and cohesive services that can be used by IT consumers, through self-service offerings including a service brokerage of external service providers.

This shift requires a different level of collaboration with IT consumers (Agencies) and TxDCS's partners. In an MSI environment with outsourced services, the visibility of the processes, shared frameworks and traceability become even more important, and shared accountability must be closely governed.

The following diagram depicts the drivers and the challenges that the Agencies and TxDCS are facing, and have set out to address.



In order to fulfill the needs of the business and to respond to the new market drivers, TxDCS has developed a Hybrid-Cloud Strategy to specifically address process automation, which will in turn drive the standardization of processes and technologies, and align the internal and external providers and its people through “extreme collaboration and sharing”.

The Hybrid-Cloud strategy addresses key components of the process automation in the quest for achieving the new business goals – Provisioning, Change Management, and Remediation across On-Premise and Cloud data centers.

Provisioning

Automated provisioning, which can include self-service provisioning, is the ability to deploy an information technology service by using pre-defined procedures that are carried out electronically without requiring human intervention.

In the current setting, provisioning is a manual process which requires the assistance of several people in several roles and involves multiple paper-based steps. It could take days to move a request from the submission phase through the actual activation of service. Automating provisioning allows customers to set up and make changes to information technology services directly themselves as allowed through a web browser interface. This approach enables a more efficient and rapid response to business requests and reduces service activation and service change times to hours or in some cases minutes.

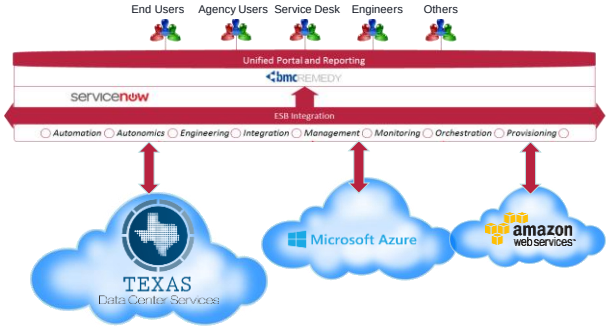
Automated provisioning is a type of policy-based management where provisioning rights can be granted on either a permissions-based or role-based basis. Once automated provisioning has been implemented, it will be up to the DIR, MSI and the Service Provider to ensure that operational processes are being followed and governance policies are in place so that the available services can evolve with the needs of the business and the availability of new types of resources and services on the market.

The design and implementation of automated provisioning requires several fundamental building blocks – these are detailed in sections included in this document. The key building blocks are as follows:

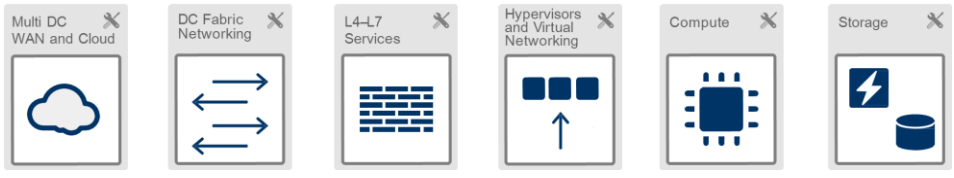
- **Catalog -** a catalog of available services and resources that can be selected individually or in bundles of resources and services by customers, depending on their needs. This catalog will be developed by the MSI, called the DCS “Marketplace”. The Marketplace Catalog will be analogous to typical internet based shopping (i.e. Amazon) with the list of available items to be

selected, pricing, and the shopping cart. For example, developers will be able to select a test server, submit the order, and within hours or minutes receive confirmation that their selected server has been "delivered" and is ready for the next step – installation of their application and database for testing.

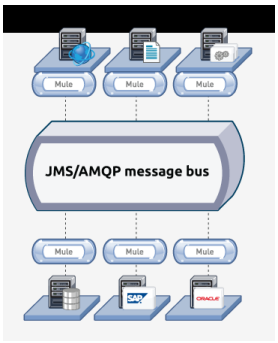
- **Requests** - A Centralized system that will translate customer provisioning orders from the Marketplace into approved requests. This system will be within the existing MSI environment. Requests will then flow from Marketplace Catalog to a system that orchestrates requests to the various providers of resources and services.
- **Cloud Resource Provisioning** – ServiceNow will act as the cloud resource orchestration system – to act on requests received from Marketplace, and in turn to provision the resources and services from the Private Cloud as well as from external or Public Clouds. In this case, the Private Cloud will be the compute and storage resources available within the TxDCS On-Premise data centers. Public Clouds will initially include AWS services (Amazon) and Azure services (from Microsoft). As the Cloud landscape changes, ServiceNow provisioning allows for rapid additions and removal of Cloud providers, and Cloud resources available in the Catalog.



- **Virtual Data Center** ("VDC", or also called "VMDC") – an important component of the Hybrid-Cloud strategy is the VDC. The VDC is required to abstract the various hardware components into known, standardized, and easily consumable data center resources. The VDC layer allows private and public compute, storage, network and security resources to be "virtualized" so that the provisioning and use of resources can be consumed more quickly, more efficiently and in a standardized fashion. For example, if the customer selection includes the requirement of a firewall, ServiceNow (the cloud resource orchestration layer) will interact with the VDC to request that firewall services be set up for a specific server or application. The SP is currently deploying VDC capabilities within the TxDCS On-Premise data center environment.



- **Enterprise Service Bus (ESB)** – the ESB is a system that enables communication between mutually interacting software applications in a service-oriented architecture (SOA). It is a set of rules and principles for integrating numerous applications together over a bus-like infrastructure. The core concept of the ESB architecture is that different applications are integrated by putting a communication bus between them and then enable each application to talk to the bus.



This ESB decouples applications and systems from each other, allowing them to communicate without dependency on or knowledge of other systems on the bus, thus moving away from "point to point" direct interactions that will be less scalable and manageable over time. For example, the DCS Orchestration layer will communicate with the VDC layer via the Enterprise Service Bus. The Service Provider is currently deploying the MuleSoft AnyPoint ESB within the TxDCS environment.

Change and Release Management

Once a cloud resource such as a virtual server on AWS has been requested and ready for deployment, the change management process kicks in. Change Management is inherently in place to protect systems, applications, data, and processes from being impacted by changes made to the environment. By reducing the risk to the business, there is often a tradeoff with the speed and flexibility at which resources can be deployed and consumed. Therefore, it is important to consider Change Management as part of the automation journey, and as closely linked to the automating of the provisioning process, it will play a key role in moving TxDCS along the Operational Maturity Model.

Change Management Process

Change approvals can be automated to a certain degree - it is rare that a proposed change is not similar to changes made in the past. The change manager would normally develop a change model to standardize the procedure for implementing a specific type of change. This streamlines the process and reduces the risk of change. Similarly, a standard change is a special case of a change model and applies to routine changes involving little risk. Standard changes are pre-approved, meaning that they do not have to be reviewed by change management and are typically treated as service requests by the service desk. These will now be automated as part of the journey along the Operational Maturity Model.

Automating of Change Management will be accomplished with key building blocks including ServiceNow, MuleSoft ESB, Remedy, and the Virtual Data Center (VDC) components.

The ServiceNow orchestration system will interact with the Change Management process supported by Remedy to automate certain changes – for instance to automate specific change approvals based on established policies and governance. This will help expedite changes, yet will allow change management to continue to protect business processes.

Remediation

Incident and Problem management processes are also key targets for automation, with the potential for significant improvement of service quality and performance, and for optimization and reduction in IT costs. The approach is simple – it is focused on knowledge and autonomics. To address Incident Management optimization, the Service Provider will deploy IPsoft's IPcenter solution – IPcenter is an ITIL-aligned service management platform that leverages autonomics to increase efficiency and quality. The initial deployment will focus on Incident Management.

IPcenter comes with a large knowledge base of incidents that have been collected by years of learning from hundreds of customer environments – the areas cover compute, storage, network, security, Operating Systems, Databases, Middleware and the list goes on. Associated with these recorded incidents are remediation tasks that have successfully resolved

these incidents. IPcenter comes with an Autonomics engine that helps make the best choice of remediation for incidents - IPSoft calls this their “virtual engineer”.

Summary

In summary, this document will primarily focus on ServiceNow and IPcenter, referencing the other Hybrid-Cloud components required to achieve the Hybrid-Cloud strategy – as follows:

Operational Maturity Process	Key Hybrid-Cloud Components
Automated Provisioning of Cloud Resources	- DIR MSI (portal and catalog) - Virtual Data Center (VDC) initiative as defined in the HCI Network SSD - Enterprise Service Bus (ESB) - ServiceNow (discussed herein)
Automating Change Management	- DIR MSI’s Remedy and related modules - Virtual Data Center (VDC) - Enterprise Service Bus - ServiceNow
Automating Incident Remediation	- DIR MSI’s Remedy and related modules - Virtual Data Center (VDC) - Enterprise Service Bus - ServiceNow - IPcenter – incident remediation/autonomics

4 Overview

4.1 Value Proposition

The Service Provider has developed a strategy to integrate the existing on-premises consolidated and non-consolidated delivery into a State of Texas Hybrid Cloud that will be made up of some of existing datacenter infrastructure investments as well as new investments in technology and partnerships. This Hybrid Cloud may eventually supersede the traditional fully managed server service model currently at the forefront of the existing services or it may grow to compliment it as a companion product. Time will tell which of these will be true, but the Service Provider believes that based on the DCS customers desire to react quicker to changing business requirements, provide more multi-function use capabilities per cpu/mem allocation and the possibility of new customers needing more “a la carte” or menu based offerings, a more flexible platform is needed.

This strategy is designed to improve current customer satisfaction by providing an improved catalog of services, a new engagement model as well as involve new customers who historically would not have considered the program due to its encumbered services and program overhead. Cost factors inherent in a fully managed server model with little automation and older lifecycle applications continue to plague both the customers and the Service Provider.

This strategy moves constituents towards a more automated, on-demand, market driven price model that is not determined as much by labor costs as it is by technology implementation and speed to market based on feature development. This changes the Service Provider service model to one that is more of a product development model that will deliver results and lower total cost of ownership to the DCS customers in the long run, as agencies will have the option to choose which services to consume.

As an additional benefit in pivoting labor resources from standard admin tasks to a higher-end value-add solution, engineering capabilities increases customer satisfaction, per employee production, and possibility of additional services based on deeper follow on relationships with customers.

The Service Provider’s Orchestration/Automation provides the foundation to make the DCS Hybrid Cloud dynamic, agile, elastic, and self-healing. A successful DCS Cloud orchestration will focus on delivering consistent quality of services. Orchestration Management adds the layer of control required to achieve consistency in a DCS Cloud. Control also includes the ability to protect and secure the DCS Cloud. Unwarranted actions in a DCS Cloud cannot be tolerated, so orchestration workflows and actions must be tightly controlled.

4.2 Business Drivers

There are a large number of drivers for the HCI plan. Generally, they can be categorized into the following broad classifications.

4.2.1 Table 1: Business Drivers

Table: Business Drivers

Driver	Detail
Business Centric Integration	☒ Integration of existing and future components and services to improve business continuity and functionality ☒ Improve user experience through unification and simplification of existing technologies
Business Centric Orchestration	☒ Orchestration created to simplify and expedite Business related functions from the user perspective ☒ Linking functions like Knowledge Search with business objectives, then aligned to IT function.
Maximization of Investment	☒ Extract individual and collective value from services through integration to allow elimination of duplicative tasks and expenditures as possible.
Leverage Vendor Relationships	☒ Be able to use vendors in but not limited to “cloud services” i.e. Amazon and Microsoft to reduce costs of virtual infrastructure through simplified user interface that provides cross vendor provisioning that takes advantage of up to the moment cost factors.
Improve Business Continuity	☒ High Availability and Disaster Recovery are to be provided across vendor, platform, and cloud along business service lines to expedite continuity and recovery of business functionality, not just IT segment.
Leverage Cloud Services	☒ Enhance agility and flexibility related to IT infrastructure through sensible cloud utilization where practical ☒ Reduce vendor dependencies through simplified web standard integration with applicable security consideration to enable the State of Texas to change vendors efficiently to take advantage of market trends and savings.
Cost Reduction	☒ Reduce IT related expenditures by maximizing investments in existing and future efforts through integration and simplification of the IT stack as possible ☒ Reduce duplicative tooling and solutions ☒ Reduce Business User training through unification of the User Interface

4.3 Benefits

4.3.1 Fitting each Purpose

The cloud has delivered proven benefits for certain workloads and use cases such as project start-ups, test & development, and handling peaks and troughs in web/application traffic. However, there can be trade-offs particularly when it comes to mission critical data security and the skills required to implement traditional IT solutions in a non-traditional ecosystem. Conversely, operating solely on dedicated gear can deliver benefits for mission critical applications in terms of enhanced security, but it is of limited use for applications with a short shelf-life such as promotional events and campaigns, or any application that experiences highly variable demand patterns such as end of month or seasonal operations.

Finding a one size fits all solution for every use case is near on impossible. Customers have different sets of requirements for different types of applications, and the TxDCS Hybrid Cloud offers the solution to meeting these needs.

The TxDCS Hybrid Cloud is a holistic approach to the consumption of IT. It is about matching the right solution to the right job. Private cloud, community cloud, public/gov cloud and dedicated servers are combined with regional access and global service availability to work together as one platform. The TxDCS Hybrid Cloud minimizes trade-offs and breaks down technical barriers through integration and automation.
.

4.3.2 Modernization and Future Proofing

Making the move to the TxDCS Hybrid Cloud could be the biggest step the DCS program takes toward future proofing our customer's missions and ensuring the program moves to the forefront of innovation in the State of Texas IT services and continues to build on the spirit intended by the DCS founding legislation.

The TxDCS Hybrid cloud gives the DCS program access to cloud resources and the ability to test new technologies swiftly with the ability to plug in existing legacy infrastructure, platforms and software, the TxDCS Hybrid cloud presents DCS customers a simplified staged approach to application deployment. Support for integrated legacy applications, data sources and services allows the DCS customer base to maximize existing investments while allowing them to move more quickly towards modernized technology.

4.3.3 Speed to Market

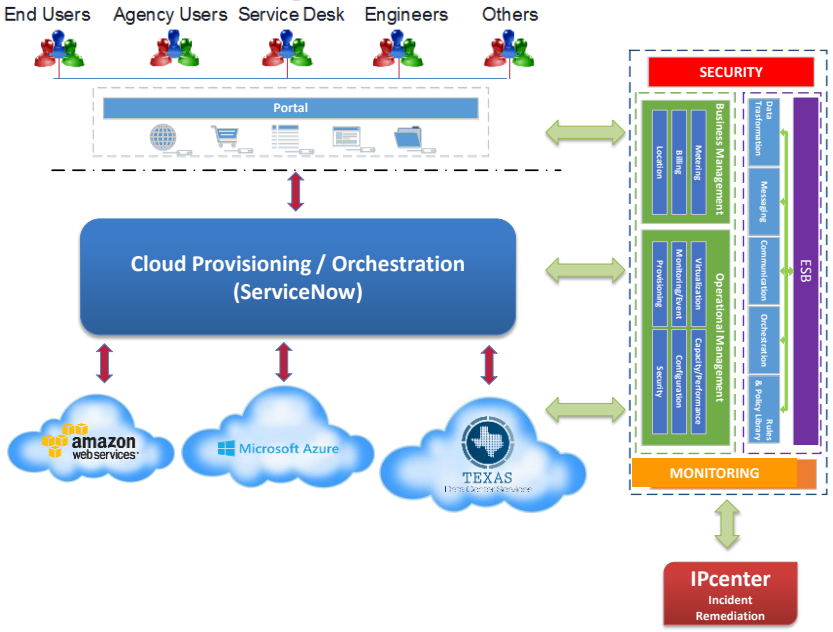
With the ability to provision cloud resources quickly and efficiently, the HCI will provide the State of Texas agencies and users with increased speed to market – developers have rapid access to required virtual environments to test and deploy applications more quickly.

5 HCI Service Integration & Orchestration (SI&O) Solution

5.1 Overview

5.1.1 Logical Solution

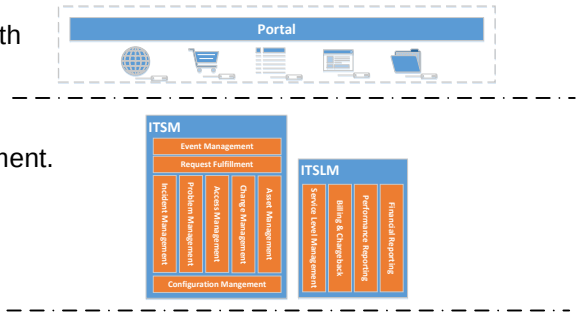
The State of Texas Hybrid Cloud solution encompasses several key components: The Hybrid-Cloud MarketPlace (Catalog and Portal), the Virtual Data Center (VDC) which abstracts the TxDCS infrastructure resources, the Cloud Resource Provisioning/Orchestration layer (ServiceNow), IPsoft's IPcenter for Incident/remediation automation, and the Enterprise Service Bus, which serves as a common, standardized communication platform for all components of the hybrid-cloud echo-system.



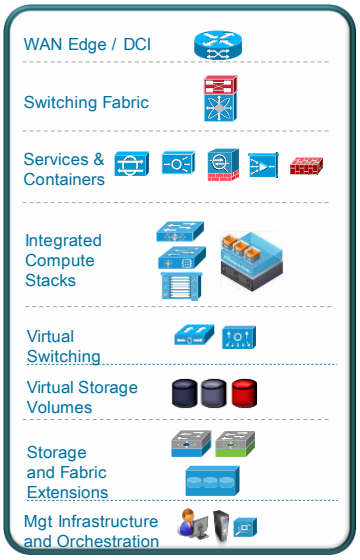
The goals of the proposed architecture are to initially automate three key processes: the provisioning of resources, change management, and the remediation of incidents – driving to increase TxDCS's Optimization along the Operational Maturity Model, and thus answering the business needs of increased business velocity and agility, and driving process and cost efficiencies.

Hybrid-Cloud Components:

The MarketPlace is composed of Remedy ARS, ITSM Suite with Service Catalog, Atrium/CMDB and associated functions and methodologies. At present DIR's MSI is in the process of being upgraded from Remedy 8x to Remedy 9x. The target for the above architecture is dependent on the Remedy 9x deployment.



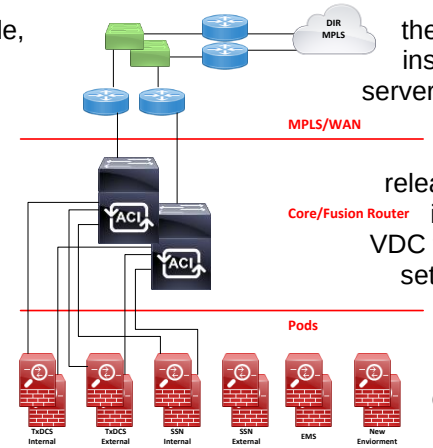
The Virtual Data Center (VDC) is composed of Virtual Hardware / Operating Systems, Network, Middleware and Storage across the State of Texas infrastructure and various Public and Private Clouds. The Service Provider has deployed VDC capabilities across the TxDCS On-Premise data centers (SDC & ADC) and intends to do so in the partner cloud environments used for HCI.



A Virtual Datacenter is a pool of cloud infrastructure resources - those resources include compute, memory, storage and bandwidth. These resources will be hosted in the private TxDCS Cloud as well as the public cloud – initially including Microsoft Azure and Amazon AWS public clouds. The VDC architecture will span multiple TxDCS data centers and public clouds.

The Virtual Data Center allows for catalogs of cloud resources so these resources can be selected and deployed quickly. Resources may include standardized resources (e.g. network ports, firewall settings, storage types and sizes), but may also include custom settings that may spawn external manual tasks as required.

For example, there may be a need to create an instance of an Agency site with web servers, a database server and specific security settings for purposes of doing testing for each application release. The security settings may include firewall rules that need to be in place. The cloud orchestration layer will interact with the VDC to automatically request and set up the necessary security settings without human intervention.



The Virtual Datacenter initially addresses the Infrastructure as a Service category of cloud resources. Enterprise Private Cloud (EPC) - As part of the TxDCS solution, the Service Provider will enable the Enterprise Private Cloud (EPC) as a dedicated and fully managed private cloud infrastructure solution - by providing a secure cloud landing zone, from which a wider hybrid cloud ecosystem can be accessed.

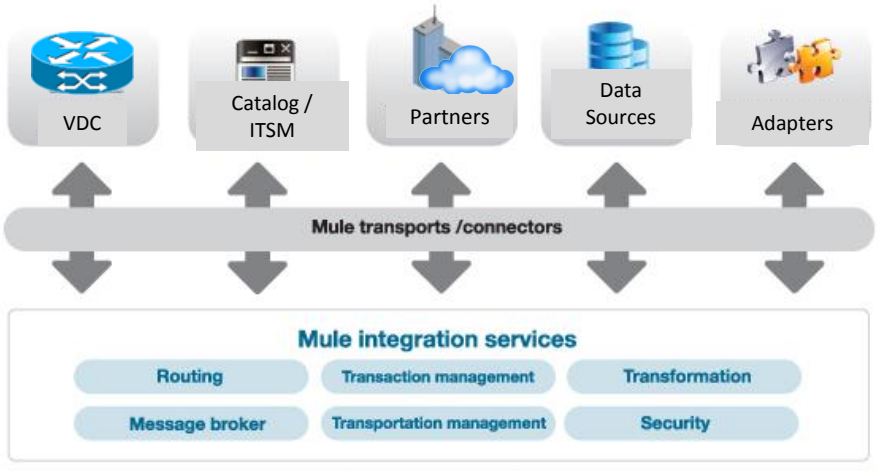
The solution delivers all essential IaaS and Private Cloud characteristics as required by the National Institute of Standards and Technology (NIST). A complete feature set, powered by industry leading VMware, EMC and VCE technologies, is supported by comprehensive Service Provider Managed Services, consisting of infrastructure and operational services.

The Enterprise Service Bus (ESB) is the underlying fabric that allows all components of the Hybrid-Cloud architecture to communicate with each other in a standard, common method, in XML format using either the Java Message Service (JMS) or the Advanced Message Queuing Protocol (AMQP). The Service Provider will use MuleSoft AnyPoint for the Service Bus.

The Java Message Service (JMS) API is a Java Message Oriented Middleware for sending messages between two or more clients. JMS is a part of the Java Platform and is a messaging standard that allows application components based on the Java Enterprise Edition (Java EE) to create, send, receive, and read messages. It allows the communication between different components of a distributed application to be loosely coupled, reliable, and asynchronous. XML is a non-proprietary means to represent data and JMS facilitates the transport of XML documents.

NIST - [NIST Cloud Computing Reference Architecture]

JMS provides a set of interfaces for sending and receiving messages, providing a means to create loosely-coupled communication systems. JMS not only answers the XML transport question, but it does so as a Java API, thus shortening the learning curve. With XML the old concerns about whether data adheres to various systems and business partner's conventions are reduced.



In the proposed Hybrid-Cloud architecture it is the intent that systems communicate via the ESB, for certain core tasks. For example, when provisioning certain tasks related to cloud workloads, the Cloud Provisioning / Orchestration layer (ServiceNow's Service Catalog) will need to know what IP address to give a Cloud Compute Resource (e.g. a virtual machine). ServiceNow will therefore interact with the Virtual Data Center to request an IP address, via the ESB functionality in a standardized, common format. Thus, the underlying hardware, software and services can change over time, but the format and method to request the IP address (in this example) remains the same – providing flexibility to the State of Texas and its customers.

ServiceNow will provide the Cloud Resource Provisioning and Orchestration for the Hybrid-Cloud architecture. End users utilize the MarketPlace service that is constructed on the –ITSM Service Catalog to select services as required. Many of resources and services available in the Catalog will be handled directly between Remedy and the service/resource pools, via the ESB. However, for cloud resources, Orchestration and Provisioning are accomplished through integration with ServiceNow's Service Catalog as published by the Service Provider via standard Web Service API.

When called, the ServiceNow Catalog entries launch Cloud Orchestration within ServiceNow to Provision and modify virtual servers/services as associated to the individual catalog entry in a DCS VDC. Updates back to Remedy are done via standard Web Service API to Remedy ARS and ultimately to the Atrium CMDB.

Remedy will be updated via ServiceNow, which will be kept accurate with updates from the DCS tools in near real-time. This allows for an auditable flow and maintaining systems integrity.

The diagram below shows the key components of the logic architecture:

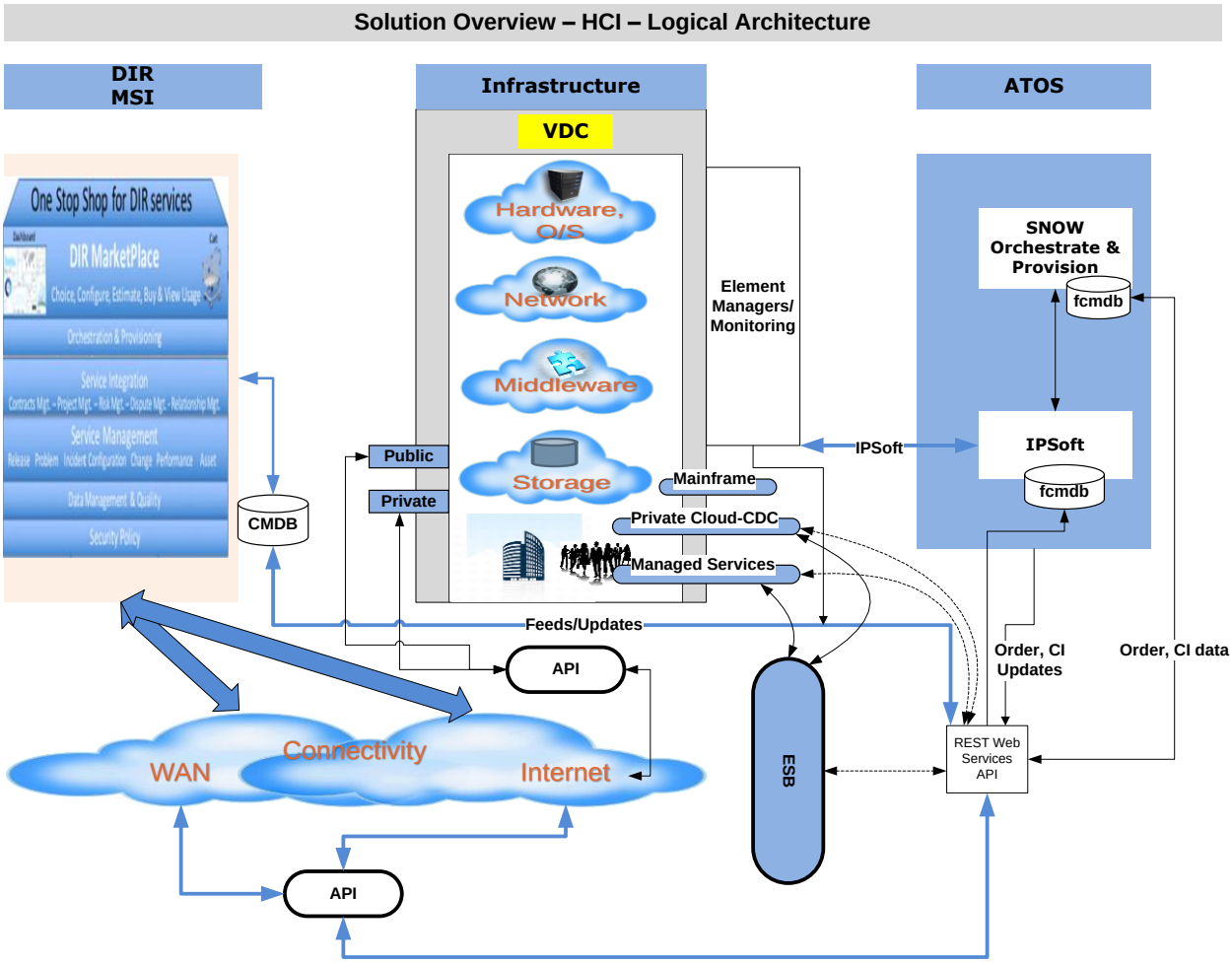
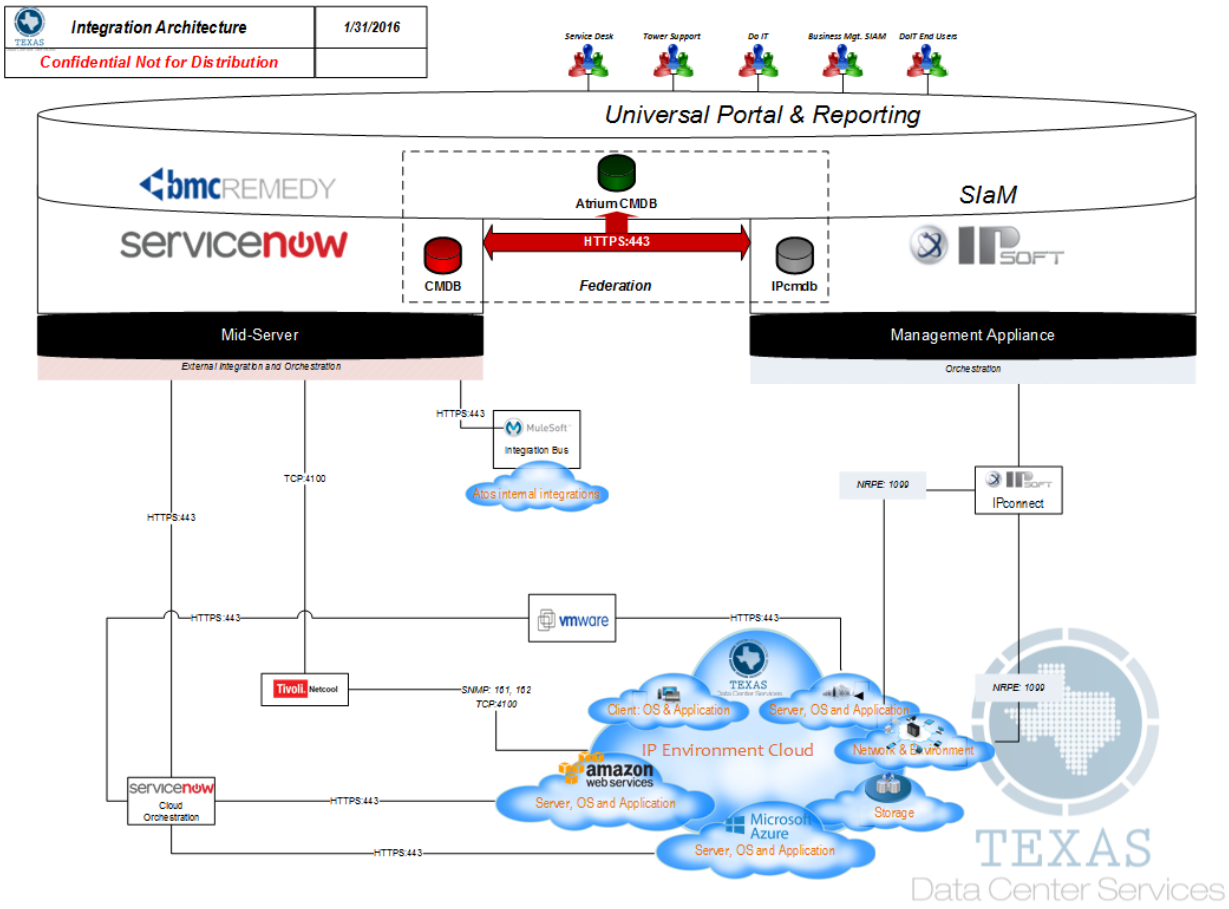


Diagram: Logical Infrastructure Architecture

BMC Remedy's Atrium CMDB is the CMDB of record with federation to ServiceNow's CMDB and IPsoft's IPcmdb. This linkage via HTTPS: 443 are essential for integrated Information Technology Service Management (ITSM), Service Integration and Management (SIaM), and Orchestration functionalities. Reconciliation is done at the Atrium level only and is done with the Remedy Reconciliation Engine. BMC Remedy and ServiceNow work together for Portal, Service Catalog, and Reporting functionality.

The following diagram shows the logical flows for ServiceNow and IPSoft components (see description below).



Note that the existing Tivoli Netcool implementation will be integrated with ServiceNow, and then expanded as required for Event Management and Discovery.

IPsoft's IPconnect provides automation delivery and handling of detected incidents through its autonomic functionality. This functionality will be initially focused on the TxDCS environment, but will be extended as opportunity arises to external clouds. IPconnect leverages a large database of incident and associated remediation solutions learned over time and allows for a more automated and rapid resolution of incidents. IPsoft will interface with the Hybrid-Cloud components via the ESB.

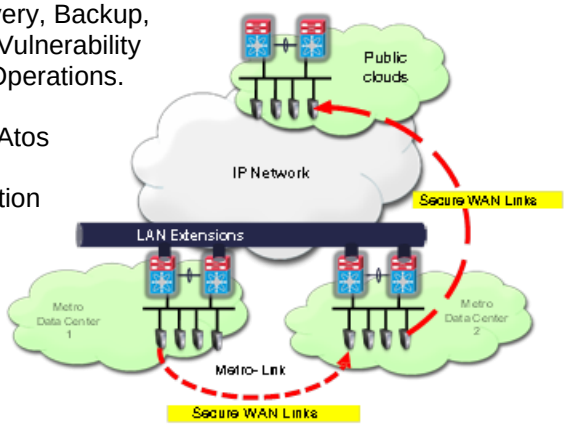
Additional details are provided in the ServiceNow and IPSoft sections below.

5.1.2 Physical Solution

The ServiceNow system will be hosted as an enhanced SaaS solution within the secure ServiceNow data centers. The enhanced SaaS solution includes a Single instance for Data, and a Single tenant infrastructure model with dedicated hardware. The environment is Certified ISO27001, SSAE16 and SOC1/Type 2 attestation.

Data in transit is protected via IP white-listing, black lists, mutual authentication, ACL's and High-Security plug-in to enable secure integrations. Utilization of Virtual Internet Protocol (VIP) addresses and port address translation. Column-level database encryption is offered using AES 128-bit, 256-bit or 3DES depending on the data and security requirements. FIPS 140-2 compliant full disk encryption is also featured. ServiceNow operates based on NIST 800-53 controls.

ServiceNow is secured with Advanced High-Availability, High-Redundancy, Disaster Recovery, Backup, Application patch management, a Vulnerability Management program, and 24x7 Operations.

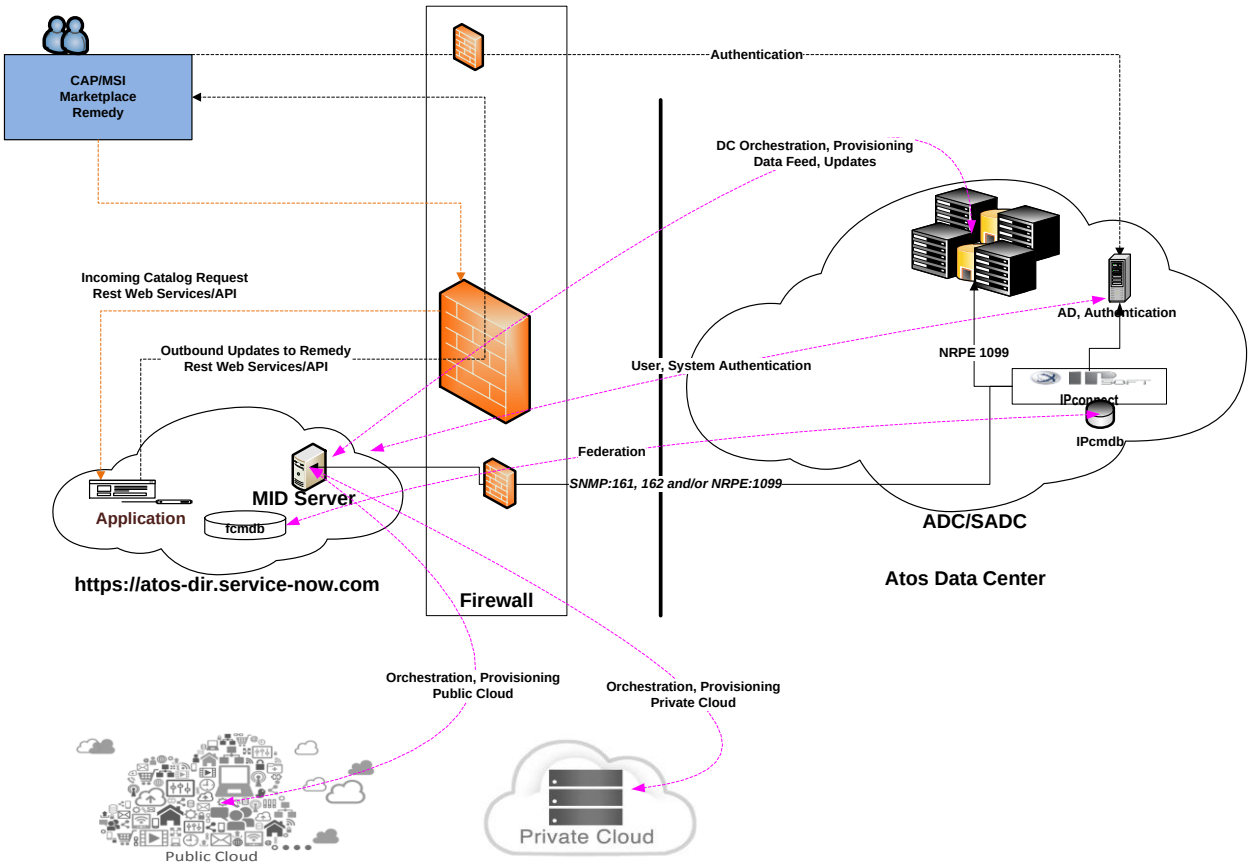


ServiceNow (SNOW) – Provisioning and Orchestration
- Integration with HCI components via API's, direct and/or via the ESB
- An enhanced SaaS solution hosted by ServiceNow (dedicated instance)
- Secure communication and encrypted data at rest and in transit

Ipcenter – automation of incident remediation
- Integration with HCI components via the ESB
- Hosted in Atos data center
- Secure communication

IPcenter will be housed within the Atos Data Centers (On-Premise configuration) and provide automation delivery and handling of detected incidents through its virtual agent functionality. Updates and patches are made available from the IPsoft support site and will be applied by Service Provider engineers. Patches that relate to components deployed that is functionally relevant to the deployment i.e. security patching or knowledge updates, will be downloaded and then applied to the components as required during a scheduled maintenance window or as an emergency change as directed by the Change Review Board (CRB) as part of the agreed upon change process.

Solution Overview – HCI – Physical Architecture



5.2 Solution Features

5.2.1 ServiceNow

ServiceNow for Brokerage and Orchestration
ServiceNow (SNOW) will provide the ability to provision private and public cloud resources:

- SNOW to DIR Marketplace (Remedy) integration – Requests will flow from the Marketplace to SNOW, and in turn SNOW will directly provision private and multiple public clouds based on business rules provided by the Marketplace.

- Business rules managed by the Marketplace in alignment with business needs (e.g. time / location / compliance / data requirements / purpose) will be translated into requests to SNOW, so that SNOW can automatically provision the requested resources and environments.

- SNOW will provide information back to Remedy - providing visibility into usage, capacity, price, performance - providing discrete detail associated to catalog items, as well as cost associated with catalog exceptions.

- SNOW will be supported with Full lifecycle management of services along with intake of new services into the catalog from Conceptualize to Design, Validate, Build, Deployment, Operate, and eventually to Retire.

Advanced High Availability (AHA)
ServiceNow's data centers and cloud-based infrastructure have been designed to be highly available. All servers and network devices have redundant components and multiple network paths to avoid single points of failure.

At the heart of this architecture, each customer application instance is supported by a multi-homed network configuration with multiple connections to the Internet. Production application servers are load balanced within each data center. Production database servers are replicated in near-real time to a peer data center within the same geographic.

ServiceNow leverages AHA for customer production instances in several ways:

- In the event of the failure of one or more infrastructure components, service is restored by transferring the operation of customer instances associated with the failed components to redundant infrastructure.

- Before executing required maintenance, ServiceNow proactively transfers operation of customer instances impacted by the maintenance to redundant infrastructure. The maintenance then proceeds without impacting service availability. This approach means that the transfer between active and standby infrastructure is being regularly executed as part of our standard operating procedures – ensuring that when it is needed to address a failure, the transfer will be successful and service disruption minimized. Through ServiceNow's unique, multi-instance architecture, Advanced High Availability meets and exceeds stringent requirements surrounding data sovereignty, availability and performance. Production database servers are replicated in near-real time to a peer data center within the same geographic region

Advanced High Availability Architecture - ServiceNow's data centers are arranged in pairs. ServiceNow has 8 data center pairs (for a total of 16 data centers) across four geographic regions. Within the US region, there are specific pairs for each U.S. customer production data is stored in both data centers and kept in sync using asynchronous database replication. The data centers to be utilized for the State of Texas are located in Texas (Primary) and Virginia (Secondary).

Both data centers are active at all times, each with the ability to support the combined production load of the pair. A production instance from one customer may be operating out of one data center in the pair and a production instance of another customer from the other. ServiceNow maintains continuous, asynchronous replication from the database in the current primary data center (read-write) to the secondary data center (read-only).

To transfer a customer instance from a primary data center to a secondary, ServiceNow designates the secondary to be the primary and the primary to be the secondary if it still exists. High-Level Overview of AHA Process

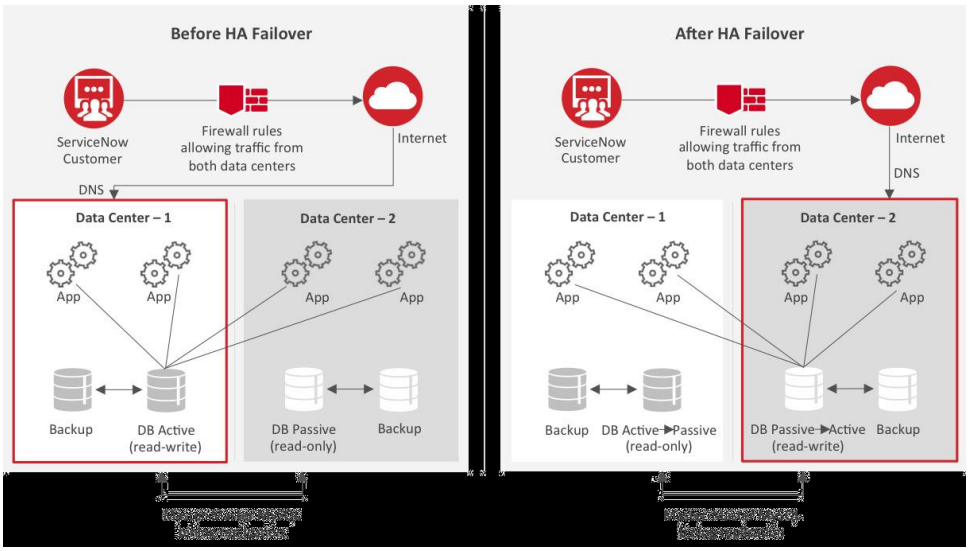
The AHA process is invoked through ServiceNow's Service Automation Platform in one of two conditions:

1. In the event of a service disruption, the ServiceNow operations team determines whether a failover1 is required.

2. For scheduled maintenance activity, the ServiceNow operations team determines if an AHA transfer2 should be performed.

Failover:

1. Unplanned operation to reverse the roles for each database from active (read-write) to passive (read-only) and vice versa and repoint nodes to address an emergency situation to prevent a customer-impacting outage.
2. Transfer: Planned operation to reverse the roles for each database from active (read-write) to passive (read-only) and vice versa and repoint nodes appropriately to the new active database. The Advanced High Availability process is comprised of eight main steps and is invoked through ServiceNow's Service Automation Platform.



ServiceNow Advanced HA Before and After

In the event an AHA failover is required, some of the above steps are bypassed, as the active instance may not be accessible. In both the AHA transfer and AHA failover scenario, the cloud automation platform will make the customer instance in the peer data center active.

Backup and Recovery. While Advanced High Availability is the primary means to recover data and restore service in the case of a service disruption, in certain cases it is desirable to use ServiceNow's more

traditional data backup and recovery mechanism. This data backup and recovery system works in concert with AHA and acts as a secondary recovery mechanism.

ServiceNow stores production instances in two geographically separate regional data centers, with sub-production instances hosted in a single data center. Backups of the two production databases and the single sub-production database are taken each day for all instances throughout the private cloud infrastructure. The backup cycle consists of four weekly full backups and the past 6 days of daily differential backups that provide 28 days of backups. All backups are written to disk, no tapes are used and no backups are sent off site. All the controls that apply to live customer data also apply to backups. If data is encrypted in the live database then it will also be encrypted in the backups. Regular, automated tests are run to ensure the quality of backups. Any failures are reported for remediation within ServiceNow.

This data backup and recovery system works in concert with AHA and acts as a secondary recovery mechanism.

5.2.2 IPsoft (IPcenter)

IPcenter is an automation platform – it is an ITIL-aligned service management platform that leverages autonomics to increase efficiency and quality. IPcenter is a tool to automate reactive handling of simple incidents, basic chores, housekeeping tasks and simple changes. It enables reducing manual effort on incident and event management from monitoring, housekeeping tasks, and changes.

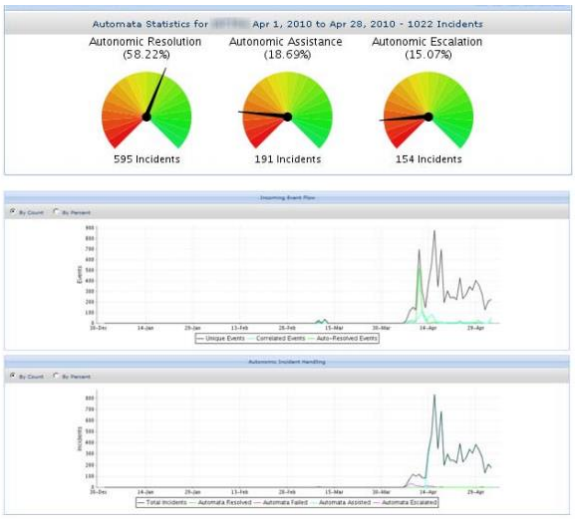
The tools receives, recognizes and resolves common / known issues on a 24/7 basis – essentially handling common level 1 and level 2 incidents. IPcenter also provides additional situational information on more complex events when escalating to technical experts (e.g. L3 admins)

The benefits are 1) improved time to response & 2) first time right in resolving incidents. IPcenter will interface with the environment via the Netcool product (to receive alerts), and will interface with Remedy for ticketing.

Initially IPcenter is focused internally within TxDCS environment and will utilize the Virtual Engineer functionality – for automating incident remediation. Virtual Engineer is the name used by IPsoft for their ability to automate tasks. Other functions within IPcenter can be extended as desired in future efforts.

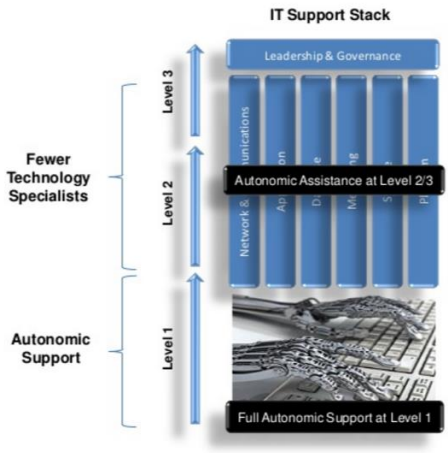
IPcenter essentially provides a cadre of “virtual engineers”. Much like human engineers, they can interact to one another and work together to resolve complex, dynamic incidents. IPcenter is able to process various types of events without any human intervention, reducing the time required of human engineers.

Autonomics work by automating the interaction between different tools that are in use within the TxDCS environment. It adapts and learns based on the successful execution of activities to and adds to the library of incidents and associated remediation solutions.



IPcenter will be able to absorb the complexity of dealing with the large increase in data and able to process information in a fraction of the time it would normally take a human engineer.

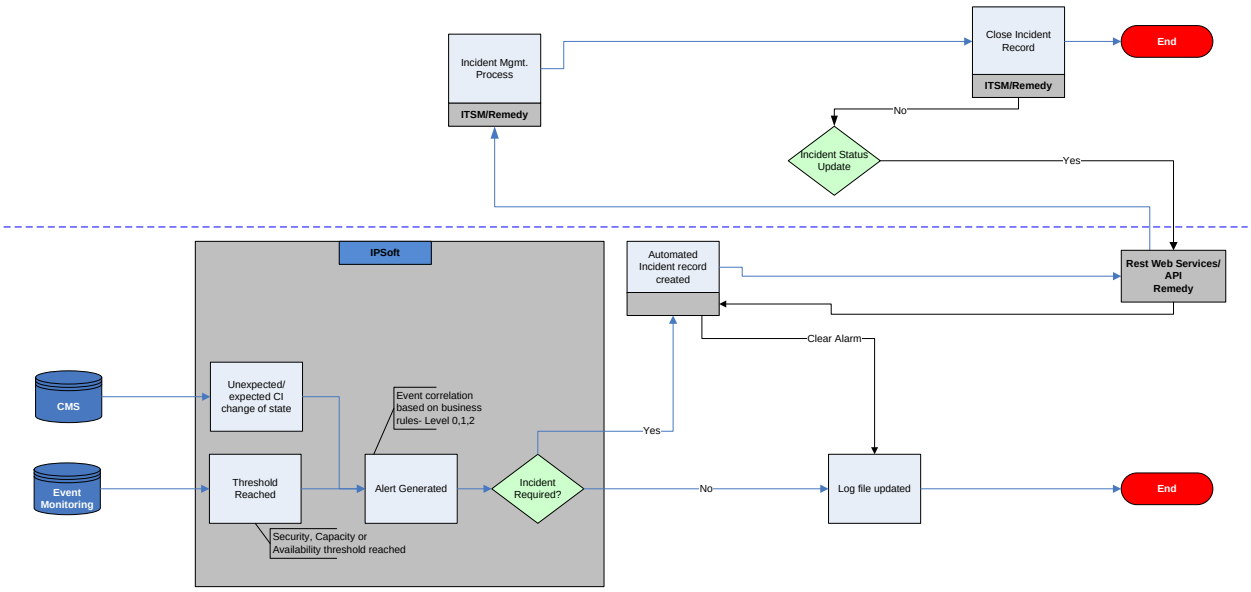
End-to-End Automation: IPcenter provides a consolidated end-to-end automation framework for addressing alerts and resolving incidents. Even when automation cannot completely remediate a problem, it can support human engineering activities by gathering information (e.g. and provide this information to a level 3 engineer to improve the time to resolution).



IPsoft (IPcenter) will be hosted within the TxDCS and provide automation delivery and handling of detected incidents through its virtual Engineer functionality.

Incident Remediation – IPcenter is comprised of a large database of knowledge including incidents and various potential resolutions and remediation solutions. Events trigger Incidents which are sent to IPcenter Virtual Agent. The Virtual Agent then determines what the best remediation action(s) might be to resolve an Incident. IPcenter then automatically triggers a suggestive response that "spawns" scripts or actions to other systems to resolve the incident. For example, an event indicating that a port might require a reset would spawn a process to request a switch to reset the port in question along with any required change management or configuration management.

IPcenter will receive events from monitoring tools and systems (see diagram below). Once a threshold or change of state of a CI is reached, and using event correlation IPsoft will determine whether an alert should be generated. IPsoft will then determine if an incident needs to be opened, and if so it will do so with Remedy. IPsoft will include the recommended remediation.



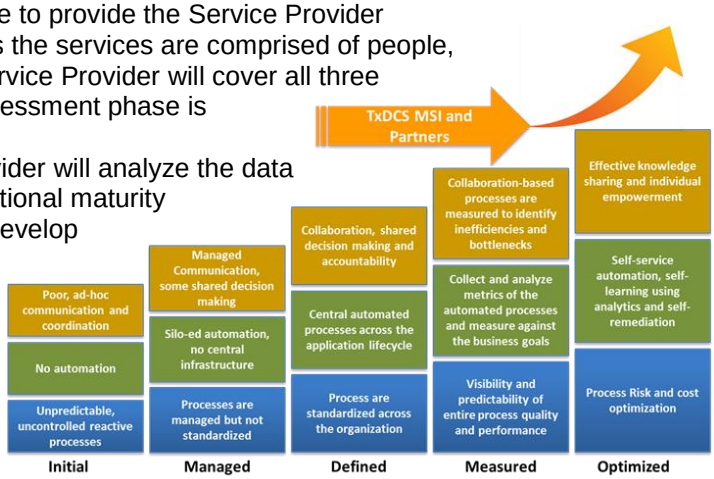
Once the most appropriate response has been selected by IPcenter's Virtual Engineer, a message is sent to ServiceNow. In turn, ServiceNow will spawn a process to automatically take action as specified, and as approved by the change management process. In some cases, the potential remediation solution(s) will be passed on to Remedy so that an actual engineer can then take appropriate action with manual intervention.

5.3 Operational Maturity Model

The State of Texas has embarked on a strategy to improve its Operational Maturity by automating a number of processes. As previously mentioned, the 3 fundamental processes that will be initially addressed through the HCI strategy are: Provisioning, Change Management and Remediation (Incident Management).

As part of MVP/Phase 1, the Service Provider will establish the Operational Maturity stream to assess, design and deploy improvements alongside the HCI deployment. The Service Provider will assess the current operational model in place by which the Service Provider provides services to the State of Texas. The Service Provider will then provide recommendations for changes and improvements, agree on those that should be completed to provide the biggest value for the change, and implement the agreed changes.

The Service Provider plans to bring in experts from our various global delivery towers to assess the processes and tools that are currently in place to provide the Service Provider contracted services to the State of Texas. As the services are comprised of people, process and associated technologies, the Service Provider will cover all three areas for each tower. The discovery and assessment phase is expected to last approximately 4 months.
After the assessment phase the Service Provider will analyze the data and based on years of experience with operational maturity models will prioritize recommendations and develop a roadmap for improving the services. The Service Provider will ensure to gather feedback and agreement with the State of Texas as to the priority, timeline and resources required by all parties for successful implementation of the agreed recommendations.



The recommendations will be closely aligned with the tools and automation streams that support these processes. The areas will cover all key towers and cross-functional services, and will include the people, process and technology components of the service. The first three processes in the following list are described in various sections above, but the Service Provider will also cover other key ITSM processes. Processes will include the following:

- Request Management
- Change Management
- Incident Management
- Capacity Management
- Problem Management
- Monitoring

As part of the deliverables, the Service Provider will document the changes in the operating procedures and will provide training to the teams that provide the support to DIR and its agencies.

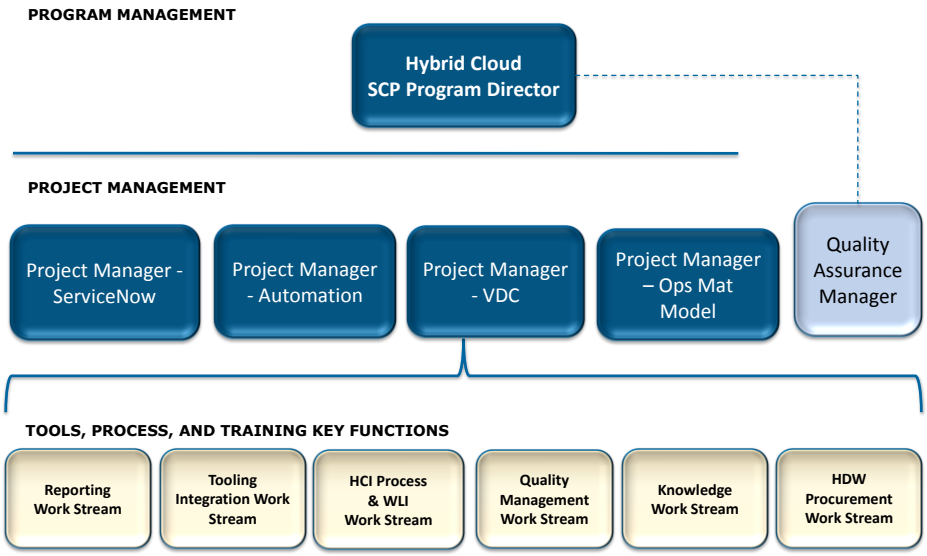
Additional details are available in the Implementation Approach section.

5.4 Implementation Approach

The Service Provider will implement the ServiceNow, IPcenter and the Operational Maturity Model initiative in 2016, starting with “Day zero” project kickoff. The Service Provider will establish a Transformation team for the HCI initiative to cover the three key components of the HCI transformation, as follows:

1. ServiceNow implementation
2. IPsoft/IPcenter implementation
3. Operational Maturity Model initiative

The project team will consist in an overall transformation project manager, with leads covering each of the three key components. Technical SME’s/Architects for ServiceNow and IPSoft will be part of the respective teams. For the Operational Maturity Model initiative, the Service Provider will bring tower leads/experts from our various global teams.



The core team will also be responsible to work closely and to integrate with other components of the HCI initiative including the VDC and Network components, the cloud providers, and the existing teams in place currently providing the services to the State of Texas. The core team will be responsible for the Future Mode of Operation (FMO) design.

The following section provides key activities for each of the 3 streams:

A. ServiceNow

a. Data Validation
b. Core Set up (ServiceNow modules, reports, dashboards, network)
c. Implementation
d. UAT / Pilot
e. Training

B. Automation (IPcenter)

a. Design and Requirements Finalized
b. Connectivity Established
c. Access Provisioned
d. Platform Deployment
e. Platform Configuration
f. Integrations (eBonding) with systems
    i. Monitoring
    ii. Ticketing
    iii. CMDB
g. IPcenter Readiness Testing
h. IPcenter User / Staff Training
i. Post Implementation Review

C. Operational Maturity Model initiative

a. Establish team - Atos service tower, tools and ITSM experts
b. Review CMO;
    i. Discovery - SOP, Inventory, Documentation of Processes, Assessment
    ii. Process-Alignment - Standardization & Globalization
    iii. KPIs and Process-Reports
    iv. HCI architecture and readiness

c. Analysis and Implementation:
    i. Set up regular Measurements
    ii. Analysis
    iii. Improvement-Proposals
    iv. Implementation
    v. Success Control
    vi. Update documentation
    vii. Training

d. Regular Audits - Evaluate the Process Maturity on ongoing basis
    i. Vision and Steering
    ii. Process
    iii. People
    iv. Technology
    v. Culture

6 Appendix

6.1 Key Assumptions

Assumption / Dependencies	Detail / Impact
Availability of Remedy 8x or 9x Environment	☒ Due to the required maintenance upgrade to the Remedy systems currently deployed, Integration is currently planned to be done with Remedy 9x, however the detailed design and implementation can also be done with version 8x, with relatively small impact. ☒ The existing Remedy components that will upgraded to 9x will stable and in production ☒ The MarketPlace via Remedy will provide logical business rules for provisioning via Service Now.
Interface	☒ Connection required between ServiceNow and Remedy will be available IP to IP https:443 fully encrypted.
Personal Information	☒ No Personally Identifiable Information will be passed from Remedy and contained within ServiceNow, unless it is encrypted. Similarly data contained in ServiceNow will be secured by the Service Provider.
CMDB	☒ Configuration Items will be maintained in ServiceNow for all Cloud Provisioned requests with relationships defined via Discovery. This CMDB information will be passed to Remedy's CMDB.
Approvals	☒ All approvals will be completed in Remedy prior to passing a cloud provisioning request to the ServiceNow system
Security	☒ Texas DIR agrees that Service Now 'Elevated' SaaS solution meets Texas DIR and agency security protocols and CJIS/FedRamp/FISMA certifications are not a requirement.
VDC	☒ VDC must be in place to support the full workload lifecycle management of public cloud resources ☒ VDC is needed for IP Addressing, DCS tools management, and security compliance and operational consistency for each DCS agency
Network Connectivity to ServiceNow	☒ Until the MPLS link(s) are in place the Service Provider will use IPSec (encrypted) VPN connectivity between the TxDCS data centers and ServiceNow data centers.
Connectivity to AWS and Azure public clouds	☒ ServiceNow will use the DCS dedicated private peering links to connect to AWS and Azure.
Enterprise Service Bus (ESB)	☒ The ESB is needed for access to the consolidated DCS tools for installation, configuration, billing, performance and capacity management of DCS services. ServiceNow and IPsoft implementation do not have a dependency on ESB for orchestration workflow execution.
Identity Management	☒ The DCS Program uses ERPM tool for privileged ID management ☒ ServiceNow and IPsoft as such do not have a dependency on Identity Management for the orchestration and provisioning of cloud resources. Identity Management information pertaining to access and provisioning of cloud workload resources is simply provided by the systems to ServiceNow, and passed on to the appropriate provisioning process.

See complete list of assumptions in Statement of Work.

6.2 Security and ServiceNow

The ServiceNow application has a wide variety of security options to choose from. Depending on the security requirements of the particular deployment, it might make sense to run the system with all of its security options enabled. Some of the options make the system more secure, but can offer additional complexity from an implementation standpoint.

High Security Settings provide these features:

- Default property values: to harden security on your platform by centralizing all critical security settings to one location for management and auditing.
- Default Deny Property: provides a security manager property to control the default security behavior for table access.
- Security Administrator Role: provides a role to prevent modification of key security settings and resources. The Security Administrator role is not inherited by the **admin** role and must be explicitly assigned.
- Elevated Privilege: allows users with the security admin role to operate in the context of a normal user and elevate to higher security role when needed.
- Property Access Control: allows security administrators to set the roles required to read and write properties.
- Transaction and system logs: are read only.
- Access Control Rules: control what data users can access and how they can access it.

High Security Settings automatically activates the Contextual Security plugin if it is not already active. In addition, Platform Security Settings - High delivers the settings and features in the context of increasing the security of the ServiceNow platform.

Additional information can be obtained from the ServiceNow Security documentation.